eSENTIRE

# Service Description:
# IR Retainer

## 1. Service Overview

eSentire's Incident Response "IR" Retainer (the "**Retainer**") entitles Client to one or more years of Retainer support (each consecutive 12-month period is a Contract Year) which will begin on the Service Commencement Date (defined on the Order Form). Client may select one of four Retainer tiers ("**Tiers**") detailed on the Order Form, and the capabilities included in each Tier are described in the sections that follow. Each Retainer Tier includes client callback, scoping call, engagement process, case management, tool deployment, threat suppression, collection and analysis of forensic artifacts, updates to client or client's counsel and written or oral reporting (these elements are "**Incident Response**").

Following the Parties' execution of an Order Form, eSentire will schedule an onboarding call with Client to collect and discuss necessary information for service setup ("**Onboarding Call**"). Depending on the Retainer Tier ordered by Client, this information may include: (a) Client contact information, including off-hours contact information and technical point of contact ("**POC**"); (b) service ordering and process for engagements; (c) a review of service level commitments and Retainer Tier options; (d) advisory service option(s); and (e) eSentire digital forensics agents (referred to as the "**eSentire Atlas Agent**" or the "**Agent**") deployment. Following the On-boarding Call, Client may begin utilizing all Retainer components relevant to the applicable Tier, though four-hour threat suppression (as applicable) will only be available when Agent software has been pre-deployed on Client endpoints in scope.

## 2. Service Definitions

In addition to the below, any capitalized terms contained in this Service Description are as defined herein.

"**Insight Portal**" means the Client interface into the Atlas Platform, where eSentire provides Client summary and detailed reporting and/or event summaries.

"**Business Email Compromise**" or "**BEC**" means one or more email accounts within the Client's email solution have been accessed by unknown parties, without authorization. Phishing email events that are not directly linked to unauthorized access to an email account within the Client's email solution are not included. A BEC is considered an urgent service event.

"**Malware Event**" means the unauthorized installation or use of software or code primarily designed to inflict harm or dysfunction on servers, workstations, security controls, data, or applications, by damaging, altering, collecting, exfiltrating or deleting data. Examples of malware include, but are not limited to, ransomware, remote access trojans, coin miners, credential stealers, viruses, worms, rootkits, keyloggers, web shells, etc. A Malware Event is considered an urgent service event.

## 3. Service Capabilities

Depending on the Retainer Tier selected by Client, the following details are around each capability available. The specifics around which Retainer Tier includes the capabilities described below and are further summarized in Section 5:

3.1 Response Times. Client may contact eSentire for both urgent and non-urgent services ("**IR Services**") by using the toll-free number ("**Hotline**") provided by eSentire during the Onboarding Call. Depending on Client's Retainer Tier, eSentire will return Client's call either on a best effort basis, or within one

hour after Client's call to the Hotline (the time to return Client's call is the "**Response Time**"). Following the call, eSentire will initiate other Incident Response activities as required. For the purposes of this section, best effort means that eSentire is not bound by any requirement to initiate Incident Response activities within any defined time frame in response to a request for Incident Response services. eSentire will only initiate Incident Response activities when the appropriate number and type of resources are available to do so.

3.2 IR Readiness Assessment. For applicable Retainer Tiers, during each Contract Year, eSentire will perform an IR Readiness Assessment (the "**Assessment**") of Client's preparedness for an incident response event. This Assessment is not considered considered an urgent service, is delivered during standard business hours, and is not subject to a Response Time. eSentire will begin to schedule and identify requirements for this Assessment during the Onboarding Call with Client and will require that the Client completes a scoping document ("**Assessment Questionnaire**"), which is used to collect information related to Client's environment. eSentire will collaborate with Client to gain an understanding of key configuration, architecture, and other information which may include the identification or collection of some or all of the following:

- Client repositories containing Client intellectual property and regulated data;
- complete list of all Client endpoints, servers, and IP addresses;
- log sources relevant to IR (to allow for optimization guidance as applicable);
- all ingress/egress points and public IP addresses;
- forensic tools that are deployed currently in Client environment;
- Client documentation outlining current IR processes and timelines;
- any special considerations; and
- patch levels on Client key servers and applications where possible.

The Assessment will include a review of information provided by Client and contained in the Assessment Questionnaire. eSentire will interview Client's internal team to understand the rules and policies that have been implemented throughout Client's environment and provide guidance on cyber security essential practices. Information will be evaluated by eSentire, and eSentire will review the results of the Assessment with Client and guide Client on the most efficient and practical actions that can be taken in the event of a security incident. The results from this Assessment will provide Client with information that will assist and expedite engaging eSentire for Incident Response activities, reducing time lost to negotiation, administration, onboarding, and forensic tool deployment when responding to an active threat. In addition to the results of the Assessment, eSentire will use the findings from this Assessment to create an incident response process RACI chart, an incident response engagement process and workflow, and a sample cyber investigation engagement letter (further described below), each of which will be reviewed with Client and posted to the Insight Portal.

The sample cyber investigation engagement letter listed above, is a sample contract, signable in the event of a security incident (the "**Cyber Investigation Engagement Letter**"). The Cyber Investigation Engagement Letter will include a general scope of investigation, and an expiration date/sign by date. The Cyber Investigation Engagement Letter created and provided by eSentire may be used by Client in the event of a cyber related emergency and will only be acted on if signed by Client on or before the expiration date. Client will have the opportunity to review the Cyber Investigation Engagement Letter and seek internal pre-approvals, so that Client may sign urgently if emergency incident support is required. Client pre-approvals may include seeking review from Client's executive team, Client counsel, and/or insurers, for example. The final Cyber Investigation Engagement Letter will also be stored in Clients Insight Portal instance, for easy access/use. After the expiration date on the Cyber Investigation

Engagement Letter, and at each Contract Year information contained in the document is subject to change, and a new Cyber Investigation Engagement Letter will be required.

All Assessment activities described in this section will run for a period of no longer than 90-Days and will be limited to five hours of eSentire support. If the Assessment activities are not completed within 90-Days (following the Retainer Onboarding Call) due to Client delays, the Assessment will be considered complete.

3.3 Advisory Service Options. For applicable Retainer Tiers, Client may select one advisory service per Contract Year, and Client may choose one from the list below. Advisory service options are not considered urgent services, are delivered during standard business hours, and are not subject to a Response Time. Client's right to one annual advisory service option does not carry over from one Contract Year to any subsequent Contract Year, and Client may change their advisory service option each Contract Year by notifying eSentire 30-Days in advance of a new Contract Year. Client acknowledges that, if Client fails to exercise such right during the time periods identified above, Client will forfeit such right with respect to that Contract Year. Options are as follows:

3.3.1 Incident Response Plan Development. If selected, eSentire will provide Client an incident response plan ("**IR Plan**") template, following the Onboarding Call, via email. The IR Plan template will contain instructions and notes to guide the Client through completion. Client will have 180 Days following receipt of the IR Plan template from eSentire, to review and complete all applicable sections. During the development, Client should save any questions it may have until completion of the template. It is the Client's responsibility to work with its legal advisors to take into consideration all applicable legal, privacy, and compliance/regulatory requirements. Sections of the IR Plan template for Client completion include (but are not limited to):

- Update Client's Full Name throughout the document;
- Version Control Section;
- Executive Sponsorship;
- Executive Leadership Titles/Roles;
- Emergency Response Threshold Guidelines;
- Contact List and War room details; and
- Link to System/Asset List.

Following completion of the draft IR Plan template, Client should send the draft IR Plan back to eSentire via email and request a review session to be scheduled. The session will be scheduled to take place over a one-hour call and is intended to work through any questions Client generated during plan completion. This call is not intended to perform an assessment of the draft IR plan or provide any content for areas that are gaps in Client's processes or procedures. Following the review call, if Client would like to schedule additional consulting time for analysis or further consulting regarding their draft IR Plan template, this can be ordered at the hourly rate, pursuant to an Engagement Letter.

3.3.2 Incident Response Plan Assessment. If selected, eSentire will request Client to send its existing IR Plan to an eSentire email (to be provided). The IR Plan must be sent to eSentire by Client no later than 180 Days following the Retainer Service Commencement Date. eSentire will confirm receipt of the IR Plan and assign a resource to conduct an assessment. eSentire will then review and assess Client's documented policies, procedures, workflows, and any other documentation included in Client's IR Plan. Within 30-Days of eSentire's receipt of Client's IR Plan, eSentire will email Client a redline to its IR Plan, which will include comments with any observations or recommendations that may assist in enhancing, maturing, or improving Client's incident response capabilities. eSentire will also offer a one-hour review call to go over the redlines sent by email. Client may use the review call to ask any

questions they may have regarding the comments or recommendations. If following the review call, Client would like to schedule additional consulting time for analysis or further consulting regarding their IR Plan, this can be ordered at the hourly rate, pursuant to an Engagement Letter.

3.3.3 Tabletop Exercise. If selected, eSentire will work with Client to develop and deliver a one-time only Incident Response Tabletop ("TTX") exercise based on the following principles:

- Senior Leadership Guidance
- Informed by Risk
- Capability-Based, Objective-Driven
- Progressive Exercise Planning Approach
- Organizational Integration

eSentire will provide a dedicated consultant throughout the TTX. This eSentire consultant will be the main point of contact and will be able to provide specific and knowledgeable guidance to Client as needed. A planning call will need to be conducted within the first 180 Days from the Retainer Service Commencement Date (unless otherwise mutually agreed). The TTX includes the following:

3.3.3.1 Planning Workshop. eSentire will host an initial workshop to establish the strategy and structure of the TTX considering the following:

- Threats & Hazards
- Areas for Improvement & Capabilities
- External Sources and Requirements
- Accreditation Standards and Regulations

3.3.3.2 Participant Identification. eSentire will work with Client to identify participants and observers who can contribute to discussions. Specific deliverables include:

- Identification and setting preparedness priorities
- Clarifying objectives and outcomes
- Identification of resources or requirements
- Identification of key personnel and stakeholders

3.3.3.3 Exercise Design and Development. eSentire will develop solid, realistic scenarios that addresses Clients' objectives.

3.3.3.4 Exercise Presentation. eSentire will facilitate the delivery of the exercises to the TTX participants.

3.3.3.5 Evaluation. eSentire will provide an effective evaluation and assess performance against exercise objectives. eSentire will identify and document strengths as well as areas for improvement relative to capabilities in an After-Action Report.

3.3.4 Dark Web Monitoring. If selected, the Dark Web Monitoring option will be provided one-time, on a non-recurring basis, and will run for a period of 30 Days. Client will be required to provide Client-specific information which will be monitored as part of the Service, which may include up to a maximum of 50 domains and executive names, and up to a maximum of 20 third party names (the "Monitored Data"). Monitored Data must be provided to eSentire by Client either within a Service onboarding worksheet ("Worksheet"), or within the eSentire Insight Portal. Over the 30-Day period, eSentire will monitor the dark web for Client Monitored Data, provide auto-alerts for credentials, typo-squatted, and potential impersonation domains, and at the end of the 30-Day period, eSentire will email a final report containing any findings (in a .PDF format). The report may include a summary of the following information (as applicable, and referred to herein as the "Findings Report"):

- Initial Access Broker, ransomware, and shell access mentions;

- Credentials being shared;
- Access to organization being sold;
- Compromised organizational data;
- Hackitivist targeting;
- Underground discussion of organization;
- Detection of open S3 buckets;
- Organizational content on GitHub;
- Relevant executive mentions;
- Relevant mentions of organization of external IP addresses on underground sites, open sources, new sites, social media/messaging platforms; and/or
- Relevant data associated with third party vendors.

Historical data will not be available for the following categories:

- Typo-squatted/potential impersonation domains; and
- Detection of open S3 buckets

3.4 Agent Deployment. For applicable Retainer Tiers, eSentire will install a cloud instance in one availability zone (Amazon data center) selected by eSentire to support Client's proximity, data residency, and/or privacy requirements, and to support Agent communications. Client is responsible for deploying the Agents in its environment. Client acknowledges Agents will require a method of deploying software throughout their organization (e.g., Intune, GPO, SCCM, PDQDeploy, etc.) and agrees to have a method reasonably satisfactory to eSentire in place prior to the Onboarding Call. Agents may be deployed to Client's Windows, macOS, or Linux computing endpoints anywhere in the world, except for embargoed countries. eSentire will provide up to two hours of support to Client to assist with such deployment at no charge; at Client's request, eSentire will provide additional support at eSentire's then-current hourly rate for such support. The eSentire Atlas Agents will sit in a warm standby state and capture critical forensic telemetry on a minimum rolling 32 consecutive day basis, which can be used by eSentire in an emergency situation if required. The number of eSentire Atlas Agents provided to Client is determined by the Retainer Tier below. Notwithstanding the Retainer Tier, in the event Client has eSentire Atlas Agent' deployed as part of another eSentire Service, the total number of eSentire Atlas Agents supported under the Retainer will mirror the number of eSentire Atlas Agents deployed as part of the other active eSentire Service leveraging such Agent. Following expiration of any Contract Year with no subsequent Renewal Term, the Agents will no longer collect telemetry, existing telemetry on the Agents will be deleted, and Client will be responsible for removing the Agents (unless Client still has another active eSentire Service leveraging eSentire Atlas Agents). Client may request additional Agents at a per/Agent fee pursuant to a signed Order Form.

3.5 Threat Suppression. Threat suppression is included in Incident Response activities. During the Retainer Term, Client may request urgent incident response services from eSentire pursuant to the processes described herein. Utilizing eSentire Agent's remote forensic analysis technology, most issues can be handled remotely through eSentire threat suppression activities ("**Threat Suppression**"). Threat Suppression includes initial analysis, beginning to identify and preserve evidence, and initiating containment measures. Threat Suppression does not mean residual malware will be fully eradicated from all systems. Complete eradication and environment remediation are outside the scope of Threat Suppression. If required, any additional remediation and forensics work following the initial Threat Suppression activities will be set forth in a separate Engagement Letter for execution by Client. In order for eSentire to perform Threat Suppression activities, Client must have completed all required Agent install activities detailed in 3.4 above. For Retainer Tiers that include a Threat Suppression guarantee,

eSentire will begin Threat Suppression activities within one hour of eSentire's receipt of an executed Engagement Letter from Client and confirmation of installation of the Agents (if not already complete). Should Client be compliant with Agent deployment and configuration requirements (see 3.4) at the time that IR Services are requested requiring Threat Suppression activities, and eSentire fails to initiate Threat Suppression within four hours of receipt of the signed Engagement Letter from Client, Client will not be responsible for fees associated with such Engagement Letter.

3.6 Hourly Rate. The committed hourly rate for Services ordered by Client pursuant to Engagement Letters is detailed on the Order Form. The hourly rate is subject to the same annual renewal term pricing increase percentage as detailed in the Order Form.

3.7 Cyber Intelligence Advisories. eSentire will provide Client with summarized threat intelligence advisories, including customer advisories of known threats, at a cadence determined by eSentire. These advisories are provided in a report format and emailed or posted to the Client's Insight Portal. Threat intelligence is not specific to any one customer, but instead is based on relevant threats to the eSentire customer base.

3.8 Threat Briefing. eSentire's threat briefing is a weekly intelligence overview provided in a report format and emailed or posted to the Client's Insight Portal. The threat intelligence team at eSentire investigates, analyzes, and organizes the most important events of the past week along with important security tips and redistributes the findings for quick reading. Information in the brief includes data that is collected and analyzed based on attempted or successful intrusions, in order to understand motives, targets and attack behavior trends.

3.9 Onsite Support. For applicable Retainer Tiers, if Client requires on-site support for urgent service requests that cannot be addressed using remote Threat Suppression or by some other reasonable means, eSentire will arrange for its personnel to travel to Client's designated location within the United States or Canada. eSentire will be in-transit within 24 hours of eSentire's receipt of an executed Engagement Letter from Client and confirmation of installation of the Agents (if not already complete).

3.10 Unlimited Incident Response. Unlimited Incident Response means delivery of all the elements of Incident Response for Qualified Events, as defined herein, an unlimited number of times throughout the Retainer Term. A "Qualified Event" is any event that occurs on Client in scope devices with an active eSentire Agent deployed on it, within the Client network that is deemed by eSentire to be a Malware or Business Email Compromise event (as defined above). All Unlimited Incident Response activities require a signed Engagement Letter (see process below). The following apply to Unlimited Incident Response:

- To qualify for Unlimited Incident Response, the following eSentire Services must be deployed and actively monitoring in the Client's environment: Endpoint Services, Network Services, Log Services, and Managed Vulnerability Service ("MVS") (together the required "**MDR Services**"). Unlimited Incident Response applies only to fully patched and properly configured Client devices which produce telemetry that eSentire continuously monitors using the MDR Services ("**Covered Devices**").
- During a response to a Qualified Event, any Incident Response Services to be performed by eSentire beyond those IR Services defined within the Unlimited Incident Response Engagement Letter will subject to a separate Engagement Letter as per the engagement process defined below.
- Client is responsible for any fees for onsite services, travel, or other sundry expenses. A request for eSentire to provide Unlimited Incident Response for a Qualified Event must be made to eSentire no later than 48 hours after Client becomes aware of such incident.

- A Malware or Business Email Compromise Event resulting from Client white-listing an endpoint, altering configurations to fall below the measured security posture, or failing to follow eSentire's prevention or remediation instructions, will not be considered Qualified Events.
- False Alarms: Should Client request that eSentire initiate Unlimited Incident Response for a Qualified Event, and eSentire determines that it was not a Qualified Event the Client agrees to pay for the time and materials consumed during the response at the Retainer Rate.
- Unlimited Incident Response does not apply to events that occurred prior to deployment of eSentire services or those events that are detected during the Onboarding Call and associated process.
- Unlimited Incident Response is limited to the provision of Incident Response Services for Qualified Events.

# 4. Engagement Process for Retainer Services

Client may contact eSentire for both urgent and non-urgent services ("**IR Services**") including incident response, threat hunting, business email compromise, forensics analysis, malcode analysis, mergers and acquisitions assessments, human resource policy/corporate security/PII/or data exfiltration investigations, data mapping, eDiscovery collection, post breach support, breach consulting, or other related security support services, by using the toll-free number ("**Hotline**") provided by eSentire during the Onboarding Call. eSentire will return Client's call after a Client call to the Hotline (see Response Times). If Client is an active eSentire Managed Detection and Response ("**MDR**") customer, the eSentire Security Operations Center ("**SOC**"), may initiate IR Services on behalf of the Client when needed, obviating the need for Client to utilize the Hotline. During the return call, or following SOC engagement, eSentire will document the requested IR Service in an Engagement Letter (a sample form will be provided to Client upon request, or during the Readiness Assessment if applicable). If Client has specific data collection and storage requirements, Client must bring these to the attention of eSentire prior to execution of the Engagement Letter. Client also must specify whether it requires any data retention. If Client fails to do so prior to execution of the Engagement Letter, eSentire will follow its standard policy, which is to delete all Client's data in its possession utilizing applicable DoD standards, including, but not limited to forensic artifacts, at the completion of the IR Services eSentire will retain administration information, written reports, and project management information, related to the Services, for two years from each Engagement Letter start date, after which point it will be deleted. Client must execute an Engagement Letter before any IR Services can commence. eSentire will invoice Client for IR Services on an hourly basis monthly in arrears at the hourly rate for the level of service selected on the Order Form (unless otherwise determined by a Qualified Event). Travel and associated expenses are not included in the hourly rate and will be invoiced separately at cost, as incurred. All work will be performed remotely unless otherwise specified.

# 5. Subscription Types

5.1. Subscriptions. Client may request a Retainer at one of four different Tiers ("**Subscription**"). The Subscription selected by Client is detailed on the Order Form, and the differences in each Subscription are identified in Table 1 below.

Table 1.

| | IR Retainer – Basic | IR Retainer – One Hour Response | IR Retainer – Threat Suppression Guarantee | IR Retainer – Unlimited IR and Threat Suppression Guarantee |
|---|---|---|---|---|
| Incident Response Activities | ✓ | ✓ | ✓ | ✓ |
| One Hour Response | | ✓ | ✓ | ✓ |
| Hourly Rate | 20% off list rate (If separate eSentire Service leveraging eSentire Atlas Agent, discount will increase to 25% off list) | 20% off list rate (If separate eSentire Service leveraging eSentire Atlas Agent, discount will increase to 25% off list) | 30% off list rate | 30% off list rate |
| Threat Briefing | ✓ | ✓ | ✓ | ✓ |
| Cyber Intelligence Advisories | ✓ | ✓ | ✓ | ✓ |
| IR Readiness Assessment | | ✓ | ✓ | ✓ |
| Onsite Support (Available US and Canada) | | ✓ | ✓ | ✓ |
| Threat Suppression Guarantee | | | ✓ | ✓ |
| Secure storage of 32 Days of forensic telemetry | | | ✓ | ✓ |
| eSentire Atlas Agents | | | ✓ (250)[1] | ✓ (250, or 1:1) [1,2] |
| One Advisory Service Option | | | ✓ | ✓ |
| Unlimited IR with MDR Services | | | | ✓ |

[1]Number of Agents may change based on other eSentire Services actively using the eSentire Atlas Agents, see section 3.4. [2]In the event Client has not received Atlas Agents as part of MDR Services, Client will be provided 250 Atlas Agents to deploy as part of this package, and necessary for Threat Suppression Guarantee.

# 5. Responsibilities and Assumptions

Client acknowledges that the ability for eSentire to deliver the Retainer and its capabilities is dependent upon Client's compliance with the responsibilities hereunder and understanding of the assumptions. In the event Client fails to perform its responsibilities herein, in the time and manner specified or contemplated below, or should any obligation set out herein with respect to the Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages.

## 5.1 Client Responsibilities:

- Scope of Service: Each Project delivered by eSentire is delivered based on agreed-upon scope as documented in an Engagement Letter or otherwise discussed, and do not include aspects beyond this scope unless explicitly stated.
- Client agrees to provide eSentire with all relevant information in its possession regarding an event throughout the course of the incident response.
- Client must provide a dedicated internal point of contact, who will be the primary point of contact for eSentire throughout the Service and will facilitate activities with Clients internal business and operation representatives.

- Response Time: Client will respond in a timely manner to urgent alerts or recommendations to ensure the efficacy of the proactive engagement.
- Client must ensure resources are scheduled and available.
- For onsite services to be performed (if applicable), Client has provided suitable workspace and necessary accesses for eSentire staff and equipment.
- Client agrees to provide eSentire with all relevant information in its possession regarding an event throughout the course of the incident response.
- Client shall reply to all document requests and other information in a timely manner and in accordance with the delivery dates established in the planning phase.

5.2 Assumptions and Terms.

- eSentire bears no liability or responsibility for losses or damages incurred by Client's third parties. Client is responsible for all actions or inactions of its third parties.
- Use of Sub-contractors. Client agrees and authorizes eSentire to use sub-contractors entirely at eSentire's discretion, to support rapid scaling of resources applied to urgent services delivery when necessary. eSentire undertakes to ensure all sub-contractor resources are properly vetted and insured prior to undertaking any work on behalf of eSentire.
- Non-urgent services will typically be performed by eSentire during regular business hours between 9am-5pm EST or outside these times by pre-arrangement.
- Incident Response activities do not guarantee specific results, including, but not limited to, complete eradication of malware, attribution to a specific individual or group of individuals, or recovery of stolen funds or data.
- In the event the number of Agents deployed as part of a Retainer Tier above, has been adjusted to match the number of Agents deployed as part of an MDR Service, and such MDR Service is not renewed (or terminates/expires), the number of eSentire Agents utilized as part of the Retainer Tier will be reverted back to the number of Agents offered as part of the Retainer Tier offering (unless Client decides to pay for additional Agents as a per/agent fee).